

Ekwan E. Rhow (CA SBN 174604)
erhow@birdmarella.com
Marc E. Masters (CA SBN 208375)
mmasters@birdmarella.com
Christopher J. Lee (CA SBN 322140)
cleec@birdmarella.com
BIRD, MARELLA, BOXER,
WOLPERT, NESSIM, DROOKS,
LINCENBERG & RHOW, P.C.
1875 Century Park East, 23rd Floor
Los Angeles, California 90067-2561
Telephone: (310) 201-2100
Facsimile: (310) 201-2110

Jonathan M. Rotter (CA SBN 234137)
Kara M. Wolke (CA SBN 241521)
Gregory B. Linkh (*pro hac vice*)
GLANCY PRONGAY & MURRAY,
LLP
1925 Century Park East, Suite 2100
Los Angeles, California 90067-2561
Telephone: (310) 201-9150
jrotter@glancylaw.com
kwolke@glancylaw.com
glinkh@glancylaw.com

Attorneys for Plaintiff Bernadine Griffith

Kalpna Srinivasan (CA SBN 237460)
Steven Sklaver (CA SBN 237612)
Michael Gervais (CA SBN 330731)
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars
14th Floor
Los Angeles, CA 90067
Telephone: (310) 789-3100
ksrinivasan@susmangodfrey.com
ssklaver@susmangodfrey.com
mgervais@susmangodfrey.com

Y. Gloria Park (*pro hac vice*)
SUSMAN GODFREY L.L.P.
1301 Ave. of the Americas
32nd Floor
New York, NY 10019
Telephone: (212) 336-8330
gpark@susmangodfrey.com

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA, EASTERN DIVISION

BERNADINE GRIFFITH, individually
and on behalf of all others similarly
situated,

Plaintiff,

vs.

TIKTOK, INC., a corporation;
BYTEDANCE, INC., a corporation,

Defendants.

CASE NO. 5:23-cv-00964-SB-E

**PLAINTIFF'S OPPOSITION TO
DEFENDANTS TIKTOK INC. AND
BYTEDANCE INC.'S MOTION TO
DISMISS PLAINTIFF'S
COMPLAINT UNDER FED. R. CIV.
P. 12(b)(6)**

Date: September 29, 2023
Time: 8:30 a.m.
Crtrm.: 6C

Assigned to Hon. Stanley Blumenfeld, Jr.

Action Filed: May 26, 2023
Trial Date: TBD

TABLE OF CONTENTS

		Page
1		
2		
3	I. INTRODUCTION.....	1
4	II. FACTUAL BACKGROUND.....	3
5	III. LEGAL STANDARD.....	4
6	IV. ARGUMENT	5
7	A. The Complaint Adequately Alleges Invasion of Privacy and	
8	Intrusion Upon Seclusion Claims.	5
9	1. Plaintiff Alleges a Reasonable Expectation of Privacy.....	5
10	2. Defendants’ Attempt to Benefit from the Disclosures of	
11	Non-TikTok Websites Fails.....	8
12	B. The CIPA Claims Survive Dismissal.....	10
13	1. Section 631: Plaintiff Alleges “Interception” In Transit.....	10
14	2. Section 632: Plaintiff Alleges “Confidential	
15	Communications.”	11
16	3. Section 632: Plaintiff Alleges that the TikTok SDK	
17	Constitutes a “Recording Device.”	13
18	C. The Complaint Adequately Alleges a CFAA Claim.	14
19	1. Plaintiff Alleges Defendants’ Trespass onto Plaintiff’s	
20	Computer.	14
21	2. Plaintiff Alleges Harm Cognizable Under the CFAA.....	14
22	D. The Complaint Adequately Alleges Statutory Larceny and	
23	Conversion Claims.....	15
24	E. The Complaint Adequately Alleges a UCL Claim.	18
25	1. Plaintiff alleges loss of property.....	18
26	2. Plaintiff alleges loss of money through the diminution of	
27	the value of her data.....	21
28	V. CONCLUSION	22

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Adler v. Community.com, Inc.</i> , No. 2:21-cv-02416-SB-JPR, 2021 WL 4805435 (C.D. Cal. Aug. 2, 2021)	12
<i>Bass v. Facebook, Inc.</i> , 394 F.Supp.3d 1024 (N.D. Cal. 2019).....	22
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007)	4
<i>Blaustein v. Burton</i> , 9 Cal.App.3d 161 (Cal. Ct. App. 1970).....	17
<i>Broidy Cap. Mgmt. LLC v. Muzin</i> , No. 19-cv-0150 (DLF), 2020 WL 1536350 (D.D.C. Mar. 31, 2020), <i>aff'd</i> , 12 F.4th 789 (D.C. Cir. 2021).....	16
<i>Brown v. Google LLC</i> , 525 F.Supp.3d 1049 (N.D. Cal. 2021).....	8, 13
<i>Brown v. Google LLC</i> , No. 20-cv-03664-LHK, 2021 WL 6064009 (N.D. Cal. Dec. 1, 2022) ..	20, 21, 22
<i>Brown v. Google LLC</i> , No. 4:20-cv-3664-YGR, 2023 WL 5029899 (N.D. Cal. Aug. 7, 2023)	<i>passim</i>
<i>Calhoun v. Google LLC</i> , 526 F.Supp.3d 605 (N.D. Cal. 2021).....	<i>passim</i>
<i>Callahan v. PeopleConnect, Inc.</i> , No. 20-cv-09203-EMC, 2021 WL 5050079 (N.D. Cal. Nov. 1, 2021)	20, 21
<i>Campbell v. Facebook, Inc.</i> , 77 F.Supp.3d 836 (N.D. Cal. 2014).....	9

1	<i>Cappello v. Walmart Inc.</i> ,	
2	394 F.Supp.3d 1015 (N.D. Cal. 2019).....	18
3	<i>CTC Real Estate Servs. v. Lepe</i> ,	
4	140 Cal. App. 4th 856 (2006).....	18
5	<i>Deering v. CenturyTel, Inc.</i> ,	
6	No. CV-10-63-BLG-RFC, 2011 WL 1842859 (D. Mont. May 16,	
7	2011).....	8
8	<i>Doe I v. Sutter Health</i> ,	
9	No. 34-2019-00258072-CU-BT-GDS, 2020 WL 1331948 (Cal.	
10	Super. Ct. Jan. 29, 2020)	17, 18
11	<i>Flanagan v. Flanagan</i> ,	
12	27 Cal. 4th 766 (2002).....	6
13	<i>G.S. Rasmussen & Assocs. v. Kalitta Flying Serv., Inc.</i> ,	
14	958 F.2d 896 (9th Cir. 1992).....	17
15	<i>Gonzales v. Uber Techs., Inc.</i> ,	
16	305 F.Supp.3d 1078 (N.D. Cal. 2018).....	19
17	<i>Hammerling v. Google LLC</i> ,	
18	615 F.Supp.3d 1069 (N.D. Cal. 2022).....	6
19	<i>hiQ Labs, Inc. v. LinkedIn Corp.</i> ,	
20	31 F.4th 1180 (9th Cir. 2022).....	14
21	<i>In re Facebook, Inc. Consumer Priv. User Profile Litig.</i> ,	
22	402 F.Supp.3d 767 (N.D. Cal. 2019).....	9, 12, 22
23	<i>In re Facebook, Inc. Internet Tracking Litig.</i> ,	
24	956 F.3d 589 (9th Cir. 2020).....	<i>passim</i>
25	<i>In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.</i> ,	
26	440 F.Supp.3d 447 (D. Md. 2020).....	18, 22
27	<i>In re Meta Pixel Healthcare Litig.</i> ,	
28	No. 22-cv-03580-WHO, 2022 WL 17869218 (N.D. Cal. Dec. 22,	
	2022)	5, 12
	<i>In re Toys R Us, Inc., Priv. Litig.</i> ,	
	No. 00-CV-2746, 2001 WL 34517252 (N.D. Cal. Oct. 9, 2001).....	14

1	<i>Jackson v. Loews Hotels, Inc.</i> ,	
2	No. ED CV 18-827-DMG, 2019 WL 6721637 (C.D. Cal. July 24,	
3	2019).....	19
4	<i>Katz-Lacobe v. Oracle Am., Inc.</i> ,	
5	No. 22-cv-04792-RS, 2023 WL 2838118 (N.D. Cal. Apr. 6, 2023).....	19
6	<i>Klein v. Facebook, Inc.</i> ,	
7	580 F.Supp.3d 743 (N.D. Cal. 2022).....	21
8	<i>Kwikset Corp. v. Superior Court</i> ,	
9	51 Cal. 4th 310 (2011).....	19, 20
10	<i>Low v. LinkedIn Corp.</i> ,	
11	900 F.Supp.2d 1010 (N.D. Cal. 2012).....	16
12	<i>Manzarek v. St. Paul Fire & Marine Ins. Co.</i> ,	
13	519 F.3d 1025 (9th Cir. 2008).....	4
14	<i>Mortensen v. Bresnan Commc’n, L.L.C.</i> ,	
15	No. CV 10-13-BLG-RFC, 2010 WL 5140454 (D. Mont. Dec. 13,	
16	2010).....	14
17	<i>People v. Gibbons</i> ,	
18	215 Cal. App. 3d 1204 (Cal App. 4th Dist. 1989).....	2, 13
19	<i>People v. Nakai</i> ,	
20	183 Cal.App.4th 499 (2010).....	6, 7
21	<i>Pruchnicki v. Envision Healthcare Corp.</i> ,	
22	845 F.App’x 613 (9th Cir. 2021).....	19, 20, 21
23	<i>Revitch v. New Moosejaw, LLC</i> ,	
24	No. 18-cv-06827-VC, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019).....	<i>passim</i>
25	<i>Saleh v. Nike, Inc.</i> ,	
26	562 F.Supp.3d 503 (C.D. Cal. 2021).....	11
27	<i>Troyk v. Farmers Grp., Inc.</i> ,	
28	171 Cal.App.4th 1305 (Cal. Ct. App. 2009).....	20
	<i>United States v. Abouammo</i> ,	
	No. 19-cr-00621-EMC-1, 2022 WL 17584238 (N.D. Cal. Dec. 12,	
	2022).....	17

1	<i>Valenzuela v. Kroger Co.,</i>	
2	No. CV 22-6382-DMG, 2023 WL 4418887 (C.D. Cal. Jun. 23,	
3	2023)	11
4	<i>Vaquero Energy, Inc. v. Herda,</i>	
5	No. 1:15-CV-0967-JLT, 2015 WL 5173535 (E.D. Cal. Sept. 3,	
6	2015)	15
7	Statutes	
8	18 U.S.C. §1030 <i>et seq.</i>	2, 14
9	Cal. Bus. & Prof. Code § 17200 <i>et seq.</i>	<i>passim</i>
10	Cal. Civ. Code §§1798.120, 1798.125	17, 19
11	Cal. Penal Code §§ 484, 496	<i>passim</i>
12	Cal. Penal Code § 630 <i>et seq.</i>	2
13	Rules	
14	Fed. R. Civ. P. 12(b)(6)	1

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Defendants—TikTok, Inc. and ByteDance, Inc.—have designed and deployed a mass surveillance system that reaches across “hundreds if not thousands of websites” to surreptitiously intercept and collect the private data of Americans. Defendants take private data from even those who have never downloaded the TikTok App and would have no reason to suspect that their private and personally identifiable data is taken by Defendants, whose data collection practices, including the sharing of data with the Chinese Communist Party (“CCP”), have been flagged as a national security threat by the U.S. government. Complaint, Dkt. 1 (“Compl.”) at ¶¶21-24, 26.

The allegations demonstrating Defendants’ impropriety are well-pleaded, and Defendants cannot escape liability for their unlawful practices by shifting blame to the websites that installed the TikTok SDK, and by distorting fact and law.

Invasion of Privacy and Intrusion upon Seclusion: Plaintiff has adequately pleaded a reasonable expectation of privacy as to her private data. Defendants’ assertion that the data taken through the TikTok SDK is not “particularly sensitive information” ignores allegations that the intercepted data includes User IDs, phone numbers, email addresses, IP addresses, search terms, and a history of all websites visited. Compl. ¶¶26, 35. The Ninth Circuit recognizes that the expectation-of-privacy inquiry focuses not only on the **nature** of the data collected but also on the **method** and **amount** of collection. *See In re Facebook, Inc. Internet Tracking Litig.* (“*FB Tracking*”), 956 F.3d 589, 602-03 (9th Cir. 2020). Here, Plaintiff alleges surreptitious method of collection by Defendants, including by circumventing browser security settings. Compl. ¶38. Plaintiff further alleges “an enormous amount of private data” collected from “millions of Americans” who visited “hundreds if not thousands of [affected] websites” that Defendants aggregate to “assemble a comprehensive profile of these non-TikTok users.” *Id.* ¶¶1, 39-42, 80. Defendants seek to evade responsibility by relying on the privacy policies of Hulu, Etsy, and Build-a-Bear to

1 argue that they have obtained consent for their practices. Yet none of these policies
 2 even mention Defendants specifically and fail to “explicitly notify” Plaintiff of
 3 Defendants’ practices at issue. *See Brown v. Google LLC (“Brown SJ”)*, No. 4:20-cv-
 4 3664-YGR, 2023 WL 5029899, at *7 (N.D. Cal. Aug. 7, 2023).

5 ***Violation of the California Invasion of Privacy Act (“CIPA”)***: Defendants
 6 incorrectly argue that Plaintiff has not alleged (i) an act of interception (for Section
 7 631) or (ii) the use of a recording device to record confidential communications (for
 8 Section 632). In fact, she has alleged both. First, Plaintiff alleges that Defendants
 9 intentionally use the TikTok SDK to read, learn, eavesdrop, record, or use electronic
 10 communications “while these electronic communications were and are in transit.”
 11 Compl. ¶98; *see Revitch v. New Moosejaw, LLC*, No. 18-cv-06827-VC, 2019 WL
 12 5485330, at *1 (N.D. Cal. Oct. 23, 2019). Second, by Defendants’ own admission,
 13 the TikTok SDK is a “piece of code” that Defendants developed to collect data. That
 14 piece of code constitutes a “recording device” under Section 632 because it was
 15 intentionally designed to, and serves no other purpose than to, collect data. *People v.*
 16 *Gibbons*, 215 Cal. App. 3d 1204, 1208 (Cal App. 4th Dist. 1989) (CIPA’s “prohibition
 17 is based on the purpose for which the device or instrument is used”). Finally, for the
 18 same reasons that Plaintiff has a reasonable expectation of privacy in her personal
 19 data, that data constitutes “confidential communications” under Section 632.

20 ***Violation of the Computer Fraud and Abuse Act (“CFAA”)***: Plaintiff
 21 adequately alleges that Defendants accessed her computer via the cookies placed on
 22 it by the TikTok SDK. Compl. ¶34. Plaintiff also alleges two different types of harm
 23 cognizable under the CFAA, including a “threat to public health and safety” posed by
 24 Defendants’ data collection that “threaten[s] to allow the [CCP] access to Americans’
 25 personal and proprietary information.” Compl. ¶¶22, 109.

26 ***Statutory Larceny and Conversion***: Defendants are wrong as a matter of law
 27 to assert that Plaintiff does not have a property interest in her private data. *See, e.g.,*
 28

1 *Calhoun v. Google LLC*, 526 F.Supp.3d 605, 635 (N.D. Cal. 2021) (collecting cases
2 recognizing property interest in private data).

3 ***Violation of California’s Unfair Competition Law (“UCL”)***: Each of the
4 foregoing violations trigger liability under the UCL. Plaintiff has standing to pursue
5 relief under the UCL because she has a property interest in her data and Defendants’
6 conduct has deprived her of that property interest and has also resulted in the
7 diminution of the value of her data. Compl. ¶¶58-61, 65-69.

8 **II. FACTUAL BACKGROUND**

9 TikTok operates a popular social-media application (the “TikTok App”), with
10 over 100 million users in the United States alone. Compl. ¶2. The TikTok App’s
11 growth has been at the expense of user privacy, and TikTok has paid out nearly \$100
12 million to settle allegations relating to their privacy violations. *Id.* at ¶¶20-21.
13 Defendants’ data collection through the TikTok App also presents national security
14 risks. *Id.* at ¶4, 22-23. The TikTok App collects private data from TikTok users and
15 transmits it to China, where companies have a legal obligation to assist the CCP with
16 information gathering. *Id.* at ¶3. Consequently, the United States has banned the
17 TikTok App on devices used by federal employees, Montana has banned the App
18 outright, and Congress is considering a nationwide ban. *Id.* at ¶¶22-24.

19 Defendants’ campaign to collect private data on unsuspecting Americans has
20 expanded to *non*-TikTok users. *Id.* at ¶5. The TikTok SDK is an insidious “piece of
21 code” developed by Defendants and marketed to websites as a way to deliver more
22 effective targeted ads. *Id.* at ¶32.¹ But Defendants also use the TikTok SDK to illicitly
23

24 _____
25 ¹ While Defendants quibble with Plaintiff’s use of the term “TikTok SDK,” Mot. 3,
26 n.2, even though that term has been used by TikTok to refer to the software at issue,
27 they do not contest Plaintiff’s description of this software as alleged in the Complaint
28 (e.g., Paragraph 5 explains that the “TikTok software owned by Defendants” is
installed on websites and “secretly intercepts and collects their private data and sends
it to Defendants”).

1 harvest a wide variety of private data from website visitors, without their consent, for
 2 Defendants’ own benefit. Defendants collect private data such as the webpages
 3 visited, search queries, User IDs, phone numbers, email addresses, IP addresses, and
 4 user agent information. *Id.* ¶¶26, 33, 36.

5 Here’s how it works: When you visit a website with the TikTok SDK installed,
 6 two cookies are downloaded onto your computer: (1) a “first-party” cookie that
 7 transmits information only to the website; and (2) a “third-party” cookie that transmits
 8 information directly to Defendants. *Id.* ¶33. Even if you configure your browser to
 9 block third-party cookies to prevent third-party tracking, “Defendants circumvent
 10 those settings to obtain Private Data anyway.” *Id.* at ¶38. The TikTok SDK does so
 11 by “causing the website to share the first-party cookie with Defendants, in effect
 12 transmuting a first-party cookie into a third-party cookie[.]” *Id.*

13 Defendants utilize the private data stolen from unsuspecting website users for
 14 a practice known as “digital fingerprinting.” Compl. ¶¶41-42. This practice involves
 15 combining private data from various sources to personally identify the website user
 16 and create a comprehensive online profile—in effect reconstructing the entirety of
 17 that website user’s traits, behaviors, and preferences as expressed through every click,
 18 every video watched, and every word searched for. *Id.* ¶¶35, 39-42.

19 The TikTok SDK is installed on numerous popular websites visited by millions
 20 of U.S. residents. *Id.* ¶43. These websites have no visible affiliation with Defendants,
 21 and website users have not consented to their web activity being transmitted to
 22 Defendants. *Id.* ¶¶26, 39.

23 **III. LEGAL STANDARD**

24 At this stage, the Court “accept[s] factual allegations in the complaint as true
 25 and construe[s] the pleadings in the light most favorable to the nonmoving party.”
 26 *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008).
 27 Plaintiff needs only allege “enough facts to state a claim to relief that is plausible on
 28 its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007).

IV. ARGUMENT

A. The Complaint Adequately Alleges Invasion of Privacy and Intrusion Upon Seclusion Claims.

A violation of privacy rights under California law requires two elements: (1) that Defendants intentionally intruded upon an area where Plaintiff had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person. *FB Tracking*, 956 F.3d at 601. Defendants challenge the sufficiency of the privacy claim only as to the first element. Mot. 5. Because privacy claims involve factual questions best left to a jury, “[c]ourts are generally hesitant to decide claims of this nature at the pleading stage.” *In re Meta Pixel Healthcare Litig.*, No. 22-cv-03580-WHO, 2022 WL 17869218, at *15 (N.D. Cal. Dec. 22, 2022).

1. Plaintiff Alleges a Reasonable Expectation of Privacy.

In *FB Tracking*, the Ninth Circuit directly addressed when an online theft of private data violates a reasonable expectation of privacy. 956 F.3d at 601-02. Yet Defendants do not even mention this binding authority. The Ninth Circuit held that the applicable test is whether “a defendant gained unwanted access to data by electronic or other covert means, in violation of the law or social norms.” *Id.* (citation omitted). The conduct at issue in *FB Tracking* was Facebook’s use of cookies to collect browsing history and search terms from non-Facebook websites. *Id.* at 596. The Ninth Circuit concluded that this method of “surreptitious and unseen” collection violated the plaintiffs’ reasonable expectation of privacy because websites utilizing the “Facebook plug-in” software downloaded cookies onto plaintiffs’ devices which continued tracking them even when they were logged out of Facebook and would not reasonably expect to be sending data to Facebook. *Id.* at 603.

Here, Defendants’ theft of private data is even more egregious. The class is not TikTok users who were merely logged out of the TikTok App at some time. This is a class of *non-users* who have “*never been registered users of the TikTok app or held any TikTok accounts.*” Compl. ¶102 (all emphases added unless otherwise noted);

1 *see id.* at ¶5. Further, the TikTok SDK uses parallel first- and third-party cookies to
 2 bypass the “block third-party cookies” and “do not track” browser settings adopted
 3 by individual users. Compl. ¶¶33-38. This circumvention is analogous to the conduct
 4 alleged in *Calhoun*, which held that plaintiffs adequately alleged a violation of their
 5 reasonable expectation of privacy where Google collected data from Google Chrome
 6 users who had activated “do not sync” browser settings. 526 F.Supp.3d at 630.

7 Defendants claim that there is a “presumption that internet communications do
 8 not reasonably give rise to an expectation of privacy.” Mot. 5. But *Brown (SJ)* recently
 9 clarified that “California courts have ***never recognized a legal ‘presumption’ that***
 10 ***internet communications are not confidential.***” 2023 WL 5029899, at *18
 11 (explaining that certain cases, including *Revitch*, have made this statement but that
 12 the assertion is misplaced because those cases “refer[red] to *People v. Nakai*, 183
 13 Cal.App.4th 499 (2010), which says nothing about a presumption”).² Defendants
 14 point to *Hammerling v. Google LLC*, 615 F.Supp.3d 1069 (N.D. Cal. 2022), but it
 15 directly refutes their claim. *Hammerling* relied heavily on *FB Tracking* to hold that
 16 individuals have a reasonable expectation of privacy in Internet communications
 17 where the data collection exceeds “common-sense expectations.” *Id.* at 1088-89. On
 18 this basis, the *Hammerling* court found that the plaintiffs ***had*** successfully alleged a
 19 reasonable expectation of privacy (even though the complaint was ultimately
 20 dismissed on other grounds). *Id.* at 1089.

21 Nor do the other cases cited by Defendants support their argument. Both *Nakai*,
 22 183 Cal.App.4th 499, and *Revitch*, 2019 WL 5485330, pre-date *FB Tracking* and
 23

24 _____
 25 ² The *Brown* court rejected this supposed “presumption” in the context of a CIPA
 26 Section 632 claim. The analysis from *Brown* is nonetheless relevant here because a
 27 communication qualifies as confidential under Section 632 if a party to that
 28 conversation has an objectively reasonable expectation of privacy in that
 conversation, i.e., that “the conversation is not being overheard or recorded.”
Flanagan v. Flanagan, 27 Cal. 4th 766, 776-77 (2002).

1 involved a narrow set of data collection limited to a single set of chat dialogues or
2 browsing activity on a single retail website. The conduct at issue in *Nakai* and *Revitch*
3 is not comparable to Defendants’ assembling “comprehensive profiles” of non-
4 TikTok users from its massive, indiscriminate, and surreptitious data collection—all
5 without the individual’s consent and, in certain circumstances, in deliberate
6 circumvention of browser privacy settings. *See* Compl. ¶¶38-39; *Brown (SJ)*, 2023
7 WL 5029899, at *20.

8 Defendants also argue that Plaintiff’s allegations are insufficient because the
9 data intercepted does not constitute “particularly sensitive information.” Mot. 6. This
10 defense-friendly spin on the allegations is false: Plaintiff alleges the theft of browsing
11 history, search queries, user IDs, phone numbers, email addresses, IP addresses, and
12 device information. *Id.* ¶¶26, 33, 36. The Ninth Circuit has found such categories of
13 data to be sensitive. *See FB Tracking*, 956 F.3d at 605 (search terms are sensitive
14 because they “could divulge a user’s personal interests, queries, and habits on third-
15 party websites operating outside of Facebook’s platform”). Further, such data not only
16 is sensitive on its own but also can be used to derive additional sensitive and
17 personally identifiable information, including what medical conditions you searched
18 for, whether you shopped for Plan B emergency contraception, whether you searched
19 for the location of an addiction treatment facility, which videos you watched, and
20 whether you have young children. *Id.* ¶¶5, 40, 75. Plaintiff also alleges that
21 Defendants can use the intercepted data to compile digital dossiers on individual users
22 through “digital fingerprinting.” *Id.* ¶¶41-42. These allegations mirror those held
23 sufficient in *FB Tracking*. *See* 956 F.3d at 604 (“allegations that Facebook allegedly
24 compiled highly personalized profiles from sensitive browsing histories and habits
25 prevent us from concluding that the Plaintiffs have no reasonable expectation of
26 privacy”).

27 Moreover, Plaintiff need not allege the exact nature of the sensitive data stolen
28 to survive dismissal. In *FB Tracking*, Facebook argued that the plaintiffs’ allegations

were insufficient because they “need to identify specific, sensitive information that Facebook collected, and that their more general allegation that Facebook acquired ‘an enormous amount of individualized data’ is insufficient.” *Id.* at 603. The Ninth Circuit disagreed, holding that courts must consider not only the *nature* of the data, but also the *method* and *amount* of collection. *Id.* The court found that the plaintiffs’ allegations were sufficient because they alleged “surreptitious and unseen” collection by Facebook through non-Facebook websites. *Id.* The same conclusion follows here, where Plaintiff alleges that “an enormous amount of private data” is collected surreptitiously by Defendants from “millions of Americans” who visited “hundreds if not thousands of [affected] websites” that is aggregated to “assemble a comprehensive profile of these non-TikTok users.” *Id.* ¶¶1, 39-42, 80; *accord Calhoun*, 526 F.Supp.3d at 630 (plaintiffs adequately alleged violation of reasonable expectation of privacy based on amount, sensitivity, and nature of data collected); *Brown v. Google LLC*, 525 F.Supp.3d 1049, 1076-77 (N.D. Cal. 2021) (same).

2. Defendants’ Attempt to Benefit from the Disclosures of Non-TikTok Websites Fails.

Defendants attempt to rely on the privacy policies of three websites visited by Plaintiff—Hulu, Etsy, and Build-a-Bear—to argue that she consented to Defendants’ data collection and thus had no reasonable expectation of privacy. Mot. 7. In all but name, Defendants assert an affirmative defense based on consent, and they carry the burden to prove a plaintiff consented explicitly. *See Calhoun*, 526 F.Supp.3d at 620.

As a preliminary matter, Defendants cite one case for their consent defense. Mot. 6. That case, *Deering v. CenturyTel, Inc.*, No. CV-10-63-BLG-RFC, 2011 WL 1842859 (D. Mont. May 16, 2011), is an unreported district court case applying Montana law which, in any event, involved more detailed disclosures regarding the data collected and with whom it was shared. *Id.* at *2.

Even if a consent defense was available to Defendants under California law, it would fail because the Hulu, Etsy, and Build-a-Bear privacy policies do not

1 “explicitly” warn users about TikTok’s specific practice of intercepting and collecting
 2 their personal data. *See Brown (SJ)*, 2023 WL 5029899, at *1 (“Because Google never
 3 explicitly told users that it [collects their data while they were browsing in private
 4 mode], the Court cannot find as a matter of law that users explicitly consented to the
 5 at-issue data collection.”); *Calhoun*, 526 F.Supp.3d at 620 (“In order for consent to
 6 be actual, the disclosures must ‘explicitly notify’ users of the practice at issue.”);
 7 *Campbell v. Facebook, Inc.*, 77 F.Supp.3d 836, 847-48 (N.D. Cal. 2014) (for a finding
 8 of consent, the disclosures must have given users notice of the “specific practice” at
 9 issue). If any reasonable user “could plausibly have interpreted the contract language
 10 as **not** disclosing . . . particular conduct,” then dismissal based on consent is not
 11 appropriate. *In re Facebook, Inc. Consumer Priv. User Profile Litig.*, 402 F.Supp.3d
 12 767, 794 (N.D. Cal. 2019) (emphasis in original).

13 Here, the websites’ privacy policies generally mention third-party data
 14 collection, but none of them specifically reference Defendants as third parties with
 15 whom data is shared. In fact, each website’s policy contains an addendum titled
 16 “About Ads,” “Cookies & Similar Technologies Policy,” or “Cookie Declaration”
 17 that enumerates the third parties that use cookies to collect information through their
 18 websites. *See* Defs.’ Request for Judicial Notice (“RJN”), Dkts. 25-6 (Hulu), 25-8
 19 (Etsy), 25-10 (Build-a-Bear). Despite disclosing over a dozen such third parties
 20 ranging from Google and Facebook to Microsoft, none of these disclosures mentions
 21 TikTok or ByteDance. *Id.*; *see* Pltf.’s Resp. to RJN (Dkt. 36). As such, the disclosures
 22 are inadequate to establish Plaintiff’s explicit consent to disclose data to Defendants.

23 Further, there is no consent (or, at a minimum, there is a disputed question of
 24 fact as to any such consent) when additional language in the privacy policy “could
 25 suggest to a reasonable user that” she could opt out of third-party data collection.
 26 *Calhoun*, 526 F.Supp.3d at 621. The Etsy, Hulu, and Build-a-Bear privacy policies
 27 are rife with such language:

- 28 ■ Etsy’s Cookie Policy states that users can “opt out of third party marketing

1 cookies and similar technologies” through the website’s privacy settings,
 2 and also “change your web browser’s settings to reflect your cookie
 3 preferences.” Dkt. 36-2.

- 4 ■ Hulu’s privacy policy states that it offers “opt-out options for third-party
 interest-based or online behavioral advertising on websites,” Dkt. 25-6.
- 5 ■ Build-a-Bear’s privacy policy states that the website is “bound by contract
 6 to refrain from using the Personal Information we collect from you for any
 7 purpose other than providing the service to Build-A-Bear Workshop.” Dkt.
 8 25-10.

9 Defendants’ consent defense relies on contractual language that is plainly insufficient
 10 to put any reasonable person on notice of the staggering amount of private data
 11 collected through the TikTok SDK.

12 **B. The CIPA Claims Survive Dismissal.**

13 Defendants argue that Plaintiff’s CIPA claims fail (1) under Section 631
 14 because there was no “interception,” (2) under Section 632 because there were no
 15 “confidential communications,” and (3) under Section 632 because there was no
 16 recording device. Defendants’ arguments lack merit.

17 **1. Section 631: Plaintiff Alleges “Interception” In Transit.**

18 Plaintiff alleges that Defendants used the TikTok SDK “to read, attempt to read,
 19 learn, attempt to learn, eavesdrop, record, and/or use electronic communications . . .
 20 *while these electronic communications were and are in transit.*” Compl. ¶98.
 21 Plaintiff also alleges in detail how Defendants use the TikTok SDK to intercept such
 22 communications. *Id.* at ¶¶32-39.

23 Ignoring these allegations, Defendants argue that Plaintiff fails to demonstrate
 24 “interception,” claiming that TikTok SDK is merely a “tool,” and “providing a tool is
 25 not an interception in transit.” Mot. 10. This argument ignores that the tool at issue
 26 was built and marketed *by Defendants* and that the data at issue is being taken *by*
 27 *Defendants* while “in transit.” Comp. ¶98. Indeed, courts have upheld similar Section
 28 631 allegations. In *Revitch*, 2019 WL 5485330, Moosejaw embedded software on its

1 webpages that allowed third-party NaviStone to scan a user’s computer. The court
 2 upheld claims against both defendants, finding that the plaintiff “adequately alleges
 3 that NaviStone acted as a third party that eavesdropped on his communications with
 4 Moosejaw because the code embedded into the Moosejaw.com pages functioned as a
 5 wiretap that redirected his communications to NaviStone while he browsed the site.”
 6 *Id.* at *1; *Saleh v. Nike, Inc.*, 562 F.Supp.3d 503, 519-21 (C.D. Cal. 2021) (upholding
 7 Section 631 claims where Nike embedded software on its webpages that allowed
 8 third-party Fullstory to capture and record user data).

9 *Valenzuela v. Kroger Co.*, No. CV 22-6382-DMG (AGRx), 2023 WL 4418887
 10 (C.D. Cal. Jun. 23, 2023), does not help Defendants. There, Judge Gee dismissed a
 11 Section 631 claim against Kroger, noting that this section “penalizes recording by a
 12 *third party*” and that Valenzuela had not identified any third party that eavesdropped
 13 on her communications with Kroger. *Id.* at *3. Here, by contrast, Defendants
 14 themselves are the third party that eavesdrops on confidential communications
 15 between Plaintiff and the websites that have installed the TikTok SDK.

16 Furthermore, Defendants’ arguments that Plaintiff has failed to plead
 17 “willfulness,” Mot. 10, are unavailing. Plaintiff alleges that “Defendants ***knowingly***
 18 ***and intentionally used*** and continue to use the TikTok SDK and receiving servers”
 19 to intercept communications. Compl. ¶98. The willfulness of Defendants’ conduct is
 20 also evident from the fact that the TikTok SDK has no other function besides
 21 intercepting communications. *See id.* at ¶¶33-36.

22 2. Section 632: Plaintiff Alleges “Confidential 23 Communications.”

24 Plaintiff has alleged that she and other class members “have an ***objectively***
 25 ***reasonable expectation of privacy*** that their private browsing communications are
 26 not being intercepted, collected or disseminated by Defendants—particularly given
 27 that Plaintiff and Class and Subclass members ***had never been registered users of the***
 28 ***TikTok app or held any TikTok accounts.***” Compl. ¶102.

1 The Court should not decide this issue in favor of Defendants at the pleading
2 stage because “whether a communication is ‘confidential’ turns on ‘numerous specific
3 factors’ and is ‘generally a question of fact.’” *Adler v. Community.com, Inc.*, No. 2:21-
4 cv-02416-SB-JPR, 2021 WL 4805435, at *5 (C.D. Cal. Aug. 2, 2021) (citation
5 omitted); *see In re Facebook*, 402 F.Supp.3d at 797 (collecting cases for proposition
6 that “[u]nder California law, courts must be reluctant to reach a conclusion at the
7 pleading stage about how offensive or serious the privacy intrusion is”). Even if the
8 Court were to decide this issue now, as demonstrated above, Defendants violated
9 Plaintiff’s objectively reasonable expectation of privacy when they surreptitiously
10 collected vast amounts of sensitive data from unsuspecting users. *See supra* at Sec.
11 IV.A.1.

12 Defendants’ cases are inapposite. In *In re Meta Pixel*, 2022 WL 17869218, the
13 court noted that the relevant question to determine the confidentiality of a
14 communication “is whether plaintiffs have shown that there is something unique
15 about these particular internet communications.” *Id.* at *14. The court held that
16 healthcare information met that standard but did not limit the scope of “confidential
17 communication” to only healthcare information. Likewise, the nature and amount of
18 data collected here is incomparable to mere “inquir[ies] about items of clothing on a
19 [single] retail website” as in *Revitch*. 2019 WL 5485330, at *3. Unlike the limited
20 data at issue in *Revitch*, the data collected here includes “search terms and a history
21 of all websites visited within Defendants’ TikTok SDK network of websites,” which
22 “allows Defendants to track the web activity of an individual and build a digital
23 dossier.” *Id.* ¶35. This data-harvesting campaign was all the more egregious because
24 of the insidious method of collection: Defendants collected data from individuals who
25 never had a TikTok account, using software embedded into websites that had no
26 visible affiliation with TikTok, and bypassed individuals’ wishes to “block third-party
27 cookies” by circumventing such settings on their browsers. The data collection here
28 is more akin to that in *Brown*, where Google “require[d] website developers to embed

Google’s code onto their websites,” did “not tell website developers that it tracks their visitors even when they are in private browsing mode,” and “t[ook] users’ private browsing history and associate[d] it with their preexisting user profiles.” 2023 WL 5029899, at *2. The Section 632 claim in *Brown* survived not only 12(b)(6) dismissal, *see* 525 F.Supp.3d at 1074, but also summary judgment, *see* 2023 WL 5029899, at *16-18.

Finally, Defendants’ assertion that there is a “general presumption against confidentiality of online communications” (Mot. 10) is incorrect and ignores *Brown*’s recent clarification that no such presumption exists. *See supra* at Sec. IV.A.1.

3. Section 632: Plaintiff Alleges that the TikTok SDK Constitutes a “Recording Device.”

Plaintiff alleges that Defendants “used and continue to use the TikTok SDK and receiving servers (where the Private Data was and is saved and recorded), ***both of which are recording devices under CIPA***, to read, attempt to read, learn, attempt to learn, eavesdrop, record, and/or use electronic communications.” Compl. ¶98. The Complaint thus directly refutes Defendants’ assertion that “there is no allegation that Defendants used a recording device.” Mot. 11. Further, in evaluating the allegations, the Court should construe “recording device” liberally, as CIPA makes “no reference . . . to a specific device or instrument,” but rather prohibits any device “***based on the purpose*** for which the device or instrument is used.” *Gibbons*, 215 Cal.App.3d at 1208. Here, regardless of the technical structure of the TikTok SDK, the Complaint alleges that the purpose of the TikTok SDK is to record electronic communications. Compl. ¶¶26, 33-36, 39.

Defendants’ last-ditch effort to appeal to legislative history, Mot. 11, is of no import at the pleading stage where the facts alleged are accepted as true. As discussed above, Plaintiff has alleged Defendants’ “use” of “the TikTok SDK and receiving servers . . . , both of which are recording devices under CIPA.” *Id.* ¶98. Defendants’

1 argument that it is “not enough” to “receive information as a result of such a device”
 2 ignores that Defendants themselves use the TikTok SDK to collect data.

3 **C. The Complaint Adequately Alleges a CFAA Claim.**

4 **1. Plaintiff Alleges Defendants’ Trespass onto Plaintiff’s** 5 **Computer.**

6 Contrary to Defendants’ claim that Plaintiff has not identified conduct “akin to
 7 breaking and entering into her computer system,” Mot. 12, the Complaint specifically
 8 alleges that “[w]hen a user visits a website that has the TikTok SDK installed, two
 9 cookies are downloaded *onto the user’s hard drive*: a ‘first-party’ cookie . . . and a
 10 ‘third-party’ cookie that is accessible directly by Defendants,” Compl. ¶33. “The
 11 ‘third-party’ cookies are downloaded *onto a user’s computing device* from each
 12 website where the TikTok SDK is installed.” *Id.* at ¶34. In short, the access alleged is
 13 Defendants’ placement of cookies on the Plaintiff’s *computer*. Defendants’ own case
 14 confirms that this pleading is sufficient to allege access in the CFAA context. *See hiQ*
 15 *Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1195 n.13, 1196 (9th Cir. 2022) (“access”
 16 in CFAA context refers to “the act of entering a computer ‘system itself’ or a
 17 particular ‘part of a computer system,’ such as files, folders, or databases”).

18 Further, Plaintiff alleges that Defendants placed cookies on her computer
 19 *without her authorization*. *See, e.g.*, Compl. ¶¶38-39, 42-43. Courts in this Circuit
 20 have long recognized that an allegation of unauthorized placement of cookies on
 21 plaintiffs’ computers is sufficient to state a CFAA claim. *See In re Toys R Us, Inc.,*
 22 *Priv. Litig.*, No. 00-CV-2746, 2001 WL 34517252, at *9 (N.D. Cal. Oct. 9, 2001);
 23 *Mortensen v. Bresnan Commc’n, L.L.C.*, No. CV 10-13-BLG-RFC, 2010 WL
 24 5140454, at *6, 8 (D. Mont. Dec. 13, 2010).

25 **2. Plaintiff Alleges Harm Cognizable Under the CFAA.**

26 Defendants misunderstand or misconstrue the Complaint to claim that Plaintiff
 27 alleges only harm to the value of her personal data. To the contrary, Plaintiff alleges
 28 a cognizable harm under the “threat to public health or safety” prong. *See* 18 U.S.C.

1 §1030(c)(4)(A)(i)(IV). Indeed, the Complaint alleges in detail recent government
 2 efforts to curb the threat posed by TikTok, including a Presidential executive order,
 3 proposed and signed congressional bills, and a state ban. Compl. ¶¶4, 22-24.

4 The reason for this governmental concern is clear: As articulated in the
 5 Presidential executive order, TikTok’s surreptitious collection of personal data
 6 “threatens to allow the Chinese Communist Party access to Americans’ personal and
 7 proprietary information—potentially allowing China to track the locations of Federal
 8 employees and contractors, build dossiers of personal information for blackmail, and
 9 conduct corporate espionage.” *Id.* at ¶22. There is no greater “threat to public health
 10 or safety” than a national security concern addressed by the office of the President.
 11 *See Vaquero Energy, Inc. v. Herda*, No. 1:15-CV-0967-JLT, 2015 WL 5173535, at
 12 *8 (E.D. Cal. Sept. 3, 2015) (recognizing harm under CFAA where Defendants’
 13 conduct adversely affected plaintiff’s “systems and computers, includ[ing] personally
 14 identifiable information and financial data of both personnel and customers”).

15 In addition, Plaintiff has separately alleged that she has suffered “out-of-pocket
 16 costs” due to Defendants’ conduct, Compl. ¶60, and that “Defendants increased the
 17 cost to Plaintiff and Class and Subclass members of mitigating the interception and
 18 collection of their Private Data by failing to notify them that Defendants were
 19 intercepting and collecting [their] Private Data,” *id.* at ¶64. These costs include paying
 20 for “McAfee security software to protect her online privacy.” *Id.* at ¶79. In short,
 21 Plaintiff incurred costs in attempting to keep her data private and will incur additional
 22 costs to do so. These costs are a “loss” recognized under Subsection (c)(4)(A)(i)(I).

23 **D. The Complaint Adequately Alleges Statutory Larceny and**
 24 **Conversion Claims.**

25 Defendants’ sole argument for dismissal of the statutory larceny and conversion
 26 counts is that Plaintiff has no property right in her “online activity data.” Mot. 14.
 27 This argument is factually and legally meritless.

28 First, as a factual matter, the Complaint alleges that Defendants stole more than

1 just “online activity data”: Defendants have developed software that “illicitly
 2 harvest[s] private and personally-identifiable data, such as the webpages visited by
 3 users, search queries, User IDs, User Agent, phone numbers, email addresses, IP
 4 addresses, and more.” Compl. ¶26. Defendants track, via third-party cookies,
 5 “individual’s unique ID number, IP address, browser screen resolution, search terms
 6 and a history of all websites visited within Defendants’ TikTok SDK network of
 7 websites.” Compl. ¶¶34-35.

8 Second, as a legal matter, Defendants’ assertion that Plaintiff enjoys no
 9 property right in her extensive private data is outdated and incorrect. Defendants
 10 principally cite *Low v. LinkedIn Corp.*, 900 F.Supp.2d 1010 (N.D. Cal. 2012), to
 11 support their argument, but they overlook more recent authorities expressly
 12 recognizing personal information as property. *Calhoun*, 526 F.Supp.3d 605, written
 13 by Judge Koh, who also authored *Low*, demonstrates the judiciary’s recognition of
 14 the changed landscape concerning the nature and value of personal information.³
 15 There, users of Google’s Chrome browser who chose not to sync their browsers with
 16 their Google accounts sued Google for collecting their personal information,
 17 notwithstanding Google’s representation that Chrome will not send users’ personal
 18 information to Google without the Sync feature turned on. *Id.* at 614-15. Google
 19 moved to dismiss the Plaintiffs’ numerous claims, including their statutory larceny
 20 claim. Judge Koh denied Google’s motion, holding that Plaintiffs “adequately alleged
 21 that they were deprived of a property interest” for purposes of a statutory larceny
 22 claim and noting the “growing trend across courts ... to recognize the lost property
 23 value of personal information.” *Id.* at 635 (collecting cases); *see Broidy Cap. Mgmt.*
 24 *LLC v. Muzin*, No. 19-cv-0150 (DLF), 2020 WL 1536350, at *16 (D.D.C. Mar. 31,
 25 2020), *aff’d*, 12 F.4th 789 (D.C. Cir. 2021) (applying California law and holding that
 26

27 ³ In *Calhoun*, Judge Koh chastised Google for doing what Defendants do here: relying
 28 on *Low* to the exclusion of “this Court’s other rulings, both before and after *Low*.”
 526 F.Supp.3d at 635.

1 electronically stored information was “property” for purposes of statutory larceny
2 claim).

3 Recent changes to California statutory law confirm personal information has
4 property value. The California Consumer Privacy Act (“CCPA”), which was enacted
5 in 2018 and took effect on January 1, 2020, “permits businesses to purchase consumer
6 information from consumers themselves ... and permits businesses to assess and
7 appraise—i.e., to place a monetary value on—consumer data.” Compl. ¶57 (citing
8 Cal. Civ. Code §1798.125). The CCPA further provides consumers with the right to
9 direct businesses to refrain from selling their personal information to third parties.
10 Cal. Civ. Code §§1798.120(a), 1798.125(a). In short, personal data now encompasses
11 “the legal right to exclude others,” which is “[a]n essential element of individual
12 property.” *Blaustein v. Burton*, 9 Cal.App.3d 161, 177 (Cal. Ct. App. 1970).

13 Ignoring this caselaw and legislation, Defendants cite three additional
14 inapposite cases. *United States v. Abouammo*, No. 19-cr-00621-EMC-1, 2022 WL
15 17584238 (N.D. Cal. Dec. 12, 2022), upheld a criminal conviction of a former Twitter
16 employee who misused a Twitter user’s confidential account information. *Id.* at *12.
17 The case has no bearing on a global corporation’s surreptitious interception and
18 collection of data from millions of consumers. If anything, the *Abouammo* court found
19 that “Twitter’s confidential user account information is ‘property’ under California
20 law.” *Id.* at *11. Defendants likewise fail to explain the relevance of *G.S. Rasmussen*
21 *& Assocs. v. Kalitta Flying Serv., Inc.*, 958 F.2d 896 (9th Cir. 1992), which involved
22 a certification scheme for alterations to airplanes, that the Ninth Circuit recognized as
23 a property right. *Id.* at 903. Finally, Defendants’ citation to *Doe I v. Sutter Health*,
24 No. 34-2019-00258072-CU-BT-GDS, 2020 WL 1331948 (Cal. Super. Ct. Jan. 29,
25 2020), is misleading. Defendants summarize the court’s recitation of a party’s
26 position, not an actual holding from the court. Mot. 15. While the *Doe I* court
27 dismissed the plaintiffs’ conversion claim, it observed that even intangible property
28 can undergird a conversion claim so long as “the property and the owner’s rights of

possession and exclusive use are sufficiently definite and certain.” *Id.* at *14.

Defendants’ cases are not persuasive against the weight of authorities reaffirming that Internet users enjoy a property interest in their personal information. *E.g., In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 440 F.Supp.3d 447, 462 (D. Md. 2020) (“For years, we have witnessed China’s voracious appetite for the personal data of Americans, including the theft of personnel records from the U.S. Office of Personnel Management [and other data breaches]. ***This data has economic value***” (quoting statement of former Attorney General William Barr)); *CTC Real Estate Servs. v. Lepe*, 140 Cal. App. 4th 856, 860 (2006) (“One’s ‘personal identifying information’ can be the object of theft. ... A person’s identifying information is a valuable asset.” (citation omitted)).

E. The Complaint Adequately Alleges a UCL Claim.

“[A] private [UCL] plaintiff must be able to show economic injury caused by unfair competition,” meaning “lost money or property.” *Cappello v. Walmart Inc.*, 394 F.Supp.3d 1015, 1019 (N.D. Cal. 2019) (citing Cal. Bus. & Prof. Code §17204). Plaintiff here has lost money or property in two ways, each of which is sufficient to establish UCL standing.

1. Plaintiff alleges loss of property.

First, Plaintiff has standing under the UCL because she has a property interest in her private data, and Defendants’ conduct has deprived her of that property and diminished its value. Compl. ¶¶65; *see id.* at ¶¶58-61, 65-69. Indeed, in *Calhoun*, the court observed that “the Ninth Circuit and a number of district courts, including this Court, have concluded that plaintiffs who suffered a loss of their personal information suffered economic injury and had standing.” 526 F.Supp.3d at 636; *see Cappello*, 394 F.Supp.3d at 1019 (plaintiffs can establish UCL standing by “hav[ing] a present or future property interest diminished”).

This caselaw is buttressed by recent changes to California law to strengthen protection for consumers’ data. As discussed above, the CCPA now provides

1 consumers with the right to direct businesses to refrain from selling their personal
 2 information to third parties. *See supra* at Sec. IV.D. In addition, voters passed the
 3 California Privacy Rights Act (“CPRA”) in November 2020, with the stated purpose
 4 of “further protect[ing] consumers’ rights, including the constitutional right of
 5 privacy.” CPRA §3. The CPRA strengthens the data protections provided by the
 6 CCPA, explaining that “[c]onsumers should know who is collecting their personal
 7 information..., how it is being used, and to whom it is disclosed,” and that
 8 “[c]onsumers should be able to control the use of their personal information.” CPRA
 9 §3(A)(1)-(2). Recently, in *Brown (SJ)*, the court rejected Google’s summary judgment
 10 motion against plaintiffs’ UCL claim, holding that “plaintiffs have identified an
 11 unopposed property interest for at least a portion of the class period under the
 12 California Consumer Privacy Act.” 2023 WL 5029899, at *21.

13 Defendants’ cases are unpersuasive. First, both *Jackson v. Loews Hotels, Inc.*,
 14 No. ED CV 18-827-DMG (JCx), 2019 WL 6721637 (C.D. Cal. July 24, 2019), and
 15 *Gonzales v. Uber Techs., Inc.*, 305 F.Supp.3d 1078 (N.D. Cal. 2018), pre-date the
 16 CCPA’s effective date and the passage of the CPRA. Second, *Katz-Lacobe v. Oracle*
 17 *Am., Inc.*, No. 22-cv-04792-RS, 2023 WL 2838118, (N.D. Cal. Apr. 6, 2023),
 18 misinterprets the elements of UCL standing as articulated in *Kwikset Corp. v.*
 19 *Superior Court*, 51 Cal. 4th 310 (2011), and improperly attempts to override Ninth
 20 Circuit and California Supreme Court precedent with district court and lower state
 21 court caselaw.⁴

22 In *Kwikset*, the California Supreme Court confirmed that a plaintiff satisfies the

23 _____
 24 ⁴ *Katz-Lacobe* cites one Ninth Circuit case, *Pruchnicki v. Envision Healthcare Corp.*,
 25 845 F.App’x 613 (9th Cir. 2021), for the proposition that misappropriation of personal
 26 information “does not establish compensable damages.” 2023 WL 2838118, at *8.
 27 *Pruchnicki* expressly recognized, however, that Plaintiff’s pleadings about
 28 misappropriated personal data “alleged sufficient injury-in-fact to support standing.”
 845 F.App’x at 614. What the pleadings did not establish was cognizable injury to
 establish compensable damages ***under Nevada law***.

1 “loss of money or property” element of the UCL where he suffers “economic injury”
 2 for Article III standing purposes. *Id.* at 322-23. Put differently, the definition of
 3 “injury in fact” under the UCL is co-extensive with “economic injury” under Article
 4 III. *See id.* at 324. And under Article III, even an “identifiable trifle” of economic
 5 injury is sufficient to establish standing. *Id.*; *see Troyk v. Farmers Grp., Inc.*, 171
 6 Cal.App.4th 1305, 1338, 1340 (Cal. Ct. App. 2009) (“The UCL requires only that the
 7 plaintiff must once have had an ownership interest in the money or property acquired
 8 by the defendant through unlawful means.” (citation omitted)).

9 In *FB Tracking*, the Ninth Circuit held that misappropriation of personal data,
 10 including plaintiffs’ browsing histories, constitutes economic injury for Article III
 11 standing purposes. 956 F.3d at 600. More specifically, *FB Tracking* held that plaintiffs
 12 sufficiently alleged “that their browsing histories carry financial value,” that they have
 13 a right to disgorgement of Facebook’s profits resulting from the misappropriation of
 14 their data, and that plaintiffs thus adequately pleaded economic injury for standing
 15 purposes. *Id.* at 600-01. Critically, the fact that plaintiffs did not “demonstrate that
 16 they either planned to sell their data, or that their data was made less valuable through
 17 Facebook’s use” did not detract from the standing analysis. *Id.* at 599. Courts in the
 18 Ninth Circuit have since repeatedly found that personal data has economic value. *See*
 19 *Brown (SJ)*, 2023 WL 5029899, at *21; *Brown v. Google LLC*, No. 20-cv-03664-
 20 LHK, 2021 WL 6064009, at *17 (N.D. Cal. Dec. 1, 2022) (plaintiffs lost money when
 21 Google took “valuable data” and “received *no* money in return” (emphasis in
 22 original)); *Callahan v. PeopleConnect, Inc.*, No. 20-cv-09203-EMC, 2021 WL
 23 5050079, at *19 (N.D. Cal. Nov. 1, 2021) (plaintiffs’ personal information is
 24 “intellectual property” for which they were not paid).

25 Here, just as in *FB Tracking*, *Brown*, and *Callahan*, Plaintiff pleaded that
 26 Defendants misappropriated her personal data, Compl. ¶¶33-38, 75-80, that her stolen
 27 data had economic value, *id.* at ¶¶44-55, and that she is entitled to disgorgement or
 28 restitution damages for the value of that data, *id.* at ¶59.

1 **2. Plaintiff alleges loss of money through the diminution of the**
 2 **value of her data.**

3 The Complaint details the existence of a “robust market” for personal data that
 4 “undergirds the tech economy.” Compl. ¶¶45-46; *id.* at ¶50. It includes specific
 5 citations that quantify the value of personal data. *Id.* at ¶46 (value of single Internet
 6 user’s data “varied from about \$15 to more than \$40”), ¶53 (in “private market[s] for
 7 Internet users’ personal information,” such information sells for “as little as \$1” or “at
 8 an average price of \$25”). The Complaint further alleges that Plaintiff’s personal data
 9 has diminished in value due to Defendants’ surreptitious collection of that data
 10 because Plaintiff can no longer bring her private data to market. *Id.* at ¶67. These
 11 allegations are sufficient to allege “loss of money.”

12 Notably, Defendants do not dispute that personal data has value or that there
 13 are markets for such data. Defendants instead note that the Complaint does not allege
 14 that Plaintiff *personally* was aware of such markets or attempted to sell her data. But
 15 this Circuit does not hold plaintiffs to such standards for UCL standing. *See Brown*,
 16 2021 WL 6064009, at *17 (allegations that there is “active market” for personal data
 17 and identification of platforms that will pay for browsing data held sufficient for UCL
 18 standing); *cf. Klein v. Facebook, Inc.*, 580 F.Supp.3d 743, 803-04 (N.D. Cal. 2022)
 19 (identifying examples of companies willing to pay users for personal information
 20 sufficient for antitrust injury).

21 Defendants’ cases are distinguishable. First, *Pruchnicki*, 845 F.App’x 613, an
 22 unpublished memorandum disposition, deals not with Article III or UCL standing, but
 23 rather with the elements of compensable damages under Nevada law. *See supra* at
 24 Sec. IV.E.1, n.4. Second, the holdings in the two 2019 *Facebook* cases are in dispute
 25 given more recent authority recognizing the lost property value of personal
 26 information. *Brown*, 2021 WL 6064009, at *17; *Calhoun*, 526 F.Supp.3d at 636;
 27 *Marriott*, 440 F.Supp.3d at 461.

28 In any event, the *Facebook* cases are distinguishable because the plaintiffs there

1 pleaded no detail to support their allegation of economic injury. *See In re Facebook*,
 2 402 F.Supp.3d 767, 784 (N.D. Cal. 2019); *Bass v. Facebook, Inc.*, 394 F.Supp.3d
 3 1024, 1040 (N.D. Cal. 2019). In contrast, Plaintiff here has alleged in detail the robust
 4 market for personal data, the value of which is “well understood and generally
 5 accepted as a form of currency.” Compl. ¶44. The Complaint even includes specific
 6 details about dollar amounts that the data could garner. Compl. ¶¶46, 50, 53.

7 **V. CONCLUSION**

8 For the foregoing reasons, this Court should deny Defendants’ Motion to
 9 Dismiss in its entirety. If the Court disagrees, Plaintiff requests leave to amend.

10
 11 DATED: September 1, 2023

Ekwan E. Rhow
 Marc E. Masters
 Christopher J. Lee
 Bird, Marella, Boxer, Wolpert, Nessim,
 Drooks, Lincenberg & Rhow, P.C.

Jonathan M. Rotter
 Kara M. Wolke
 Gregory B. Linkh
 GLANCY PRONGAY & MURRAY, LLP

Kalpana Srinivasan
 Steven Sklaver
 Michael Gervais
 Gloria Park
 SUSMAN GODFREY L.L.P.

21
 22
 23 By: /s/ Ekwan E. Rhow

24 Attorneys for Plaintiff Bernadine Griffith

CERTIFICATE OF COMPLIANCE

The undersigned counsel of record for Plaintiff Bernadine Griffith certifies that this brief contains 6,985 words, which complies with the word limit of L.R. 11-6.1.

DATED: September 1, 2023

By: /s/ Ekwana E. Rhow

Ekwana E. Rhow

Attorney for Plaintiff